Email & Electronic Communication Policy

TABLE OF CONTENTS

PURPOSE **3**

SCOPE **3**

AUDIENCE **3**

COMPLIANCE & ENFORCEMENT **3**

POLICY STATEMENTS **4**

1. *University Electronic Mail Accounts* *4*
2. *Access to E-mail* *4*
3. *Use of E-mail* *6*

VIOLATIONS AND SANCTIONS **7**

LEGAL CONFLICTS **7**

EXCEPTIONS **7**

COMMENTS **7**

RELATED DOCUMENTS **7**

REFERENCES **7**

MANDATES **7**

DOCUMENT CONTROL INFORMATION **8**

REVISION HISTORY **8**

Purpose

This policy serves to provide a guiding reference to members of the Saint Leo University community on the appropriate use, privacy, and access of electronic communications.

Scope

The scope of this Policy applies to all University electronic communication services, including stored files and other electronic means. Such services include but are not limited to e-mail, voice-mail, web portals, and chat rooms operated by the University.

Audience

The Policy applies to all Saint Leo University personnel, and contractors. The term "personnel" refers to all full-time, part-time, interns, and temporary employees hired directly by Saint Leo University and on the Saint Leo University payroll. The term “contractor” refers to anyone who is on another University’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.).

Throughout this Policy, “Saint Leo University,” “Saint Leo,” “our,” “we,” and the “University” refer to Saint Leo University. “Personnel”, “contractor”, “you” and “yours” refer to you as an employee/ representative of Saint Leo University.

This Policy applies to Saint Leo University, all wholly owned subsidiaries, subsidiaries in which Saint Leo University has a controlling interest.

Compliance & Enforcement

Compliance with this Policy is mandatory and applies to all Saint Leo University personnel and contractors globally including at any of its subsidiaries or units as well as authorized representatives.

Saint Leo University reserves the right to modify the Policy at its sole discretion.

All Saint Leo University personnel and contractors are responsible for complying with this Policy. A violation of this Policy may result in disciplinary action, up to and including termination. Violators may also be subject to legal action, including civil and/or criminal prosecution. Saint Leo University also reserves the right to take any other action it believes is appropriate based on the severity of the infraction.

This Policy also represents a statement of intent, any behavior or act violating the spirit of this Policy is also subject to disciplinary action in a fashion similar to a policy violation. Saint Leo University personnel and contractors should also note that with specific authorization and approval from senior management, there are some business programs or services which are exempt from portions of this Policy. Saint Leo University Personnel and contractors must contact their manager or supervisor if they do not understand this Policy, are unable to comply with this Policy, or have questions regarding Policy.

Policy Statements

1. University Electronic Mail Accounts

1.1. The University uses E-mail to conduct official business and therefore, every member of the University community shall be issued an electronic mail account available for his/her use in executing their role and responsibilities.

1.2. The University has a responsibility to protect student and staff rights as well as ensure the accuracy of its business processes based on E-mail correspondence. Therefore, E-mail containing official business of the University shall be addressed to the person's official University E-mail address and should not be addressed to alternative addresses. Because Saint Leo email is an official means of communications and delivery of forwarded email cannot be guaranteed, Saint Leo email prohibits forwarding of emails to accounts outside of Saint Leo University.

1.2.1.1. E-mail name addresses are generated from the user's legal name and must be unique.

1.2.1.2. E-mail addresses for faculty and staff takes the form: ***firstname.lastnameNN@saintleo.edu*** where NN represents a numerical addition to resolve duplicate names

1.2.2. E-mail distribution lists will be maintained by UTS for certain constituency groups, organizations and committees to facilitate communication among the campus community for official business purposes. The inclusion of faculty and staff in these distribution lists is mandatory

1.2.3. To distinguish between accounts and lists, distribution lists will take the form ***Org-function-location@listserv.saintleo.edu*** using the dash "-" separator instead of the period to clearly denote a list. Example, SLU-Employees-MacDill@listserv.saintleo.edu.

1.3. On termination, resignation or withdrawal, the University may terminate an individual's E-mail account, and all information not retained by the University will be deleted.

1.3.1. The University, at its discretion, may retain an archived version of the information; our standard retention period is 30 days.

1.3.2. As a matter of good security practice, accounts not active for a one year period are considered expired and will be made inactive or deleted at the discretion of the University. There may be situations where faculty sabbaticals or teaching schedules warrant longer grace periods. Arrangements for extending account expiration must be approved by the CIO.

1.3.3. It is important that the University maintain relationships with members of the community. Therefore, students completing a degree program; staff who obtain retirement and faculty who retire or obtain emeritus status shall be eligible to have their account remain active indefinitely. The University will determine the best location where this account is maintained. E.g: username@alumni.saintleo.edu

2. Access to E-mail

2.1. General Statements

2.1.1. The University retains ownership of the records resident on the technological resources covered by this policy. The University retains the right to maintain ultimate control and

authority over its technology resources, including E-mail, and to take appropriate actions to further institutional interests.

2.1.2. E-mail communications may be subject to public access under local, state, and federal law, when relevant, to discovery in civil or criminal litigation. Any such disclosure of E-mail under these conditions will be approved by the President of the University or his/her designee.

2.2. **Privacy Statements**

2.2.1. The University cannot guard the privacy of E-mail delivered to or through systems not managed by the institution. Saint Leo University prohibits the sending of any non-public student information, as defined by the student handbook, to non-official University addresses via e-mail. For information concerning secure transmissions, contact the University Technology Services.

2.3. **Individual Expectations**

2.3.1. E-mail messages are expected to be in compliance with University policies. Individuals can expect the University to follow its policies when seeking access to E-mail communications

2.3.2. Individually addressed E-mail communications may not be intercepted (read) by any third party except as noted below. Any access of individual E-mail communications other than that noted below is in violation of University policy and appropriate action will be taken as defined in section IV of this policy.

2.4. **University Requirements**

2.4.1. University officials shall have the right to access any E-mail to preserve life and ensure the safety of the University community. The President shall be notified of the access when conditions have warranted such action.

2.4.2. Under certain circumstances the Postmaster or System Administrator may, in the course of her/his professional duties, access an individual's E-mail for legitimate management or maintenance purposes (e.g. virus removal, backup, delivery resolution, etc…). The individual will be notified about the nature of the work performed under such circumstances. If at all possible, the individual will be notified prior to the work being done or otherwise as soon as possible after the work is completed.

2.4.3. The University reserves the right to inspect and remove e-mail that might contain viruses or other harmful content or otherwise interfere with the delivery of E-mail or normal operation of computer systems. It also reserves the right to filter known or suspected virus attachments in mass prior to delivery. In such cases, UTS will notify the University as to the specific filtering being applied.

2.4.4. The University reserves the right to inspect and remove e-mail that is considered an unsolicited offer otherwise known as “SPAM'.

2.4.5. If an occasion arises when a University officer or supervisor believes that access to an individual's E-mail account is required for the conduct of urgent University business, the University individual is not available, and a system administrator is required to access the individual's E-mail account, the following procedure shall be followed:

2.4.6. The University official or supervisor shall secure permission to access the E-mail account from the supervising Vice President or President of the University.

2.4.6.1. An appropriate written order of the Vice President or President shall be presented to the system administrator allowing the system administrator to proceed to access the E-mail account.

2.4.6.2. The individual whose E-mail account has been accessed will be notified as soon as possible by copy of the above referenced order

2.4.6.3. All E-mail communications and files on campus computers, accounts, and databases are University property (see II.A.1). Upon employee termination, resignation, or withdrawal, these materials remain the property of the University

3. Use of E-mail

3.1. Business Use

3.1.1. As with other University resources, e-mail is appropriately used for purposes that further the mission and goals of the University. Persons are encouraged to be good stewards of this resource and refrain from excessive participation in the use of E-mail that is not related to the business of the University. Examples of such discouraged uses include but are not limited to:

3.1.1.1. for personal commercial gain or solicitation except in cases of officially sanctioned University activities

3.1.1.2. For self-promotion in political campaigns

3.1.1.3. Participation in chain-letters.

3.2. Unlawful Use

3.2.1. Persons may not use e-mail in violation of SLU policies, local, state or federal laws. Such policies or laws may include but are not limited to:

3.2.1.1. stalking, harassment, hate speech or other unlawful activity.

3.2.1.2. fraudulent acts, including the use of a deceptive alias to disguise one's true identity.

3.2.1.3. intentional distribution of viruses (real or simulated) and other destructive or intrusive software using E-mail.

3.2.1.4. Applicable Federal laws include, but are not limited to the CAN-SPAM Act of 2003 and Computer Fraud and Abuse Act (18 U.S.C. 1030 et seq.).

3.3. Authentic Use

3.3.1. All materials sent by campus e-mail must be attributed to the individual, office, or organization sending the material.

3.4. Official University Use

3.4.1. The University will regard the SLU address as the official e-mail address for members of the SLU community.

3.4.2. Official University business among faculty, staff and students will only be directed to SLU email addresses. SLU cannot ensure appropriate use, privacy practices or availability of 3rd party email systems.

3.5. **Information Privacy**

3.5.1. Information protected by the Federal Education Rights of Privacy Act (FERPA) should not be distributed to a non-University e-mail account.

3.5.2. It is appropriate to direct students to eLion to retrieve grades, financial status and other information that is sensitive or private rather than distribute information via email.

3.5.3. There is a growing concern about the privacy of information and identity theft. It is important to respect individual's privacy and help guard against the misuse of such information. Hence, information that is sensitive or private to the individual should not be transmitted via email. This includes, but is not limited to:

3.5.3.1. social security number
3.5.3.2. birth date
3.5.3.3. driver license number
3.5.3.4. financial account numbers

Violations and Sanctions

3.6. Community members should report violations of this policy to the CIO, Director of Human Resources, or the appropriate Vice President. Violation of this policy will be assessed by the appropriate Vice President in accordance with established University procedures as defined in the student, faculty and staff handbooks.

Legal Conflicts

Saint Leo University policies were drafted to meet or exceed the protections found in existing laws and regulations, and any policy believed to be in conflict with existing laws or regulations must be promptly reported to the Saint Leo University Grand Counsel.

Exceptions

Exceptional circumstances occur from time to time. In these situations, consult Saint Leo University Security Team for guidance.

Comments

N/A

Related Documents

-

References

- Acceptable Use Policy

Mandates

- Payment Card Industry Data Security Standard

Document Control Information

Document Control Information	
Primary Contact	Darius Lewis
Version Number	1.0
Owner	*Saint Leo University Information Security Team*
Author(s)	
Approved By	
Approval Date	
Effective Date	TBD
Creation Date	February 17, 2012
Information Classification	Saint Leo University Confidential

Revision History

Revision Level	Date	Description	Change Summary
1.0	2012 January	Original	
1.1	2013 January	Annual Review	